



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,062	10/30/2001	Shell S. Simpson	10007669-1	8476

7590 11/09/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

POWERS, WILLIAM S

ART UNIT	PAPER NUMBER
----------	--------------

2134

MAIL DATE	DELIVERY MODE
-----------	---------------

11/09/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

NOV 09 2007

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/002,062
Filing Date: October 30, 2001
Appellant(s): SIMPSON ET AL.

Charles W. Griggers, Registration No. 47,283
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 7/30/2007 appealing from the Office action mailed 2/27/2007.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct. The 35 USC 112, 2nd paragraph rejection of claims 9 and 16 are withdrawn.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6151675	Smith	11-2000
---------	-------	---------

5721908	Lagarde, et al.	2-1998
---------	-----------------	--------

Schneier, Bruce; "Applied Cryptography"; 1996; John Wiley & Sons, Inc.; pages 32-33.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Objections

1. Claim 1 is objected to because of the following informalities: the claim recites the limitation "said browser" in line 4. There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 1-10, 12-16 and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,151,675 to Smith in view of US Patent No. 5,721,908 to Lagarde et al. (hereinafter Lagarde).

As to claim 1, Smith teaches:

- a. Accessing a destination web service (dynamic document conversion server) (Smith, column 5, lines 34-36).

Smith uses the Internet to communicate between the user and server, but does not expressly mention the use of a browser. However, in an analogous art, Lagarde teaches:

- b. Downloading into said browser (Lagarde, column 9, lines 10-11) web content associated with said accessed destination web service (Lagarde, column 10, lines 12-29).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the secure document transmitting of Smith with the browser of Lagarde in order to affect web server data access over the Internet as suggested by Lagarde (Lagarde, column 1, lines 15-20).

Smith as modified further teaches:

- c. Downloading a public encryption key into said browser from said accessed destination web service (Smith, column 6, lines 28-30, figure 2A and column 3, lines 27-32).
- d. Retrieving image data under control of said browser (Lagarde, column 5, lines 16-24).
- e. Encrypting said retrieved image data, wherein said downloaded public encryption key is utilized as part of said encrypting step (Smith, column 6, lines 28-30).
- f. Transmitting said encrypted image data to said accessed destination web service (Smith, column 6, lines 31-32).
- g. Decrypting said encrypted image data by said accessed destination web service, wherein a private encryption key counterpart of said public encryption key is utilized as part of said decrypting step, said private encryption key being accessible exclusively to said accessed destination web service (Smith, column 6, lines 38-40).

As to claim 2, Smith as modified teaches said retrieved image data is previously referenced to a composition associated with said user's identity (Lagarde, column 13, lines 34-40).

As to claim 3, Smith as modified teaches said accessed destination web service represents a production device (Smith, column 5, lines 7-13 and figure 1).

As to claim 4, Smith as modified teaches said production device is a printer (Smith, column 5, lines 7-13 and figure 1).

As to claim 5, Smith as modified teaches said retrieving comprises accessing said user's identity from said destination web service via said web content through an imaging extension (Lagarde, column 12, lines 29-39).

As to claim 6, Smith as modified does not expressly disclose a hard disk. However, Official Notice is given that it is well known that modern computer systems employ hard disks as secondary memory.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Smith as modified using a hard disk for secondary memory.

As to claim 7, Smith as modified teaches said image data is contained in a PDF file (Smith, column 5, lines 46-56).

As to claim 8, Smith as modified teaches choosing desired options represented by said destination web service through said web content (Lagarde, column 10, lines 37-41).

As to claim 9 as best understood by the Examiner, Smith as modified teaches securely transmitting data (Smith, column 6, lines 31-32).

As to claim 10, Smith as modified teaches creating a print job reflecting said desired options, said print job including said image data (Lagarde, column 14, line 62-column 15, line 32).

As to claim 12, Smith as modified teaches:

- a. Accessing a destination web service (dynamic document conversion server) (Smith, column 5, lines 34-36).
- b. Download web content from said destination web service to a user's browser (Lagarde, column 9, lines 10-11 and column 10, lines 12-29).
- c. Download a public encryption key from said destination web service (Smith, column 6, lines 28-30, figure 2A and column 3, lines 27-32).
- d. Encrypt imaging data using said public encryption key as part of encryption process (Smith, column 6, lines 28-30).
- e. Transmit said encrypted imaging data to said destination web service (Smith, column 6, lines 31-32).
- f. Direct said destination web service to decrypt said encrypted imaging data using a private encryption key counterpart of said public encryption key as part of decryption process, said private encryption key being accessible exclusively to said destination web service (Smith, column 6, lines 38-40).

As to claim 13, Smith as modified teaches said imaging data is previously referenced to a composition associated with a user's identity (Lagarde, column 13, lines 34-40).

As to claim 14, Smith as modified teaches said destination web service represents a production device (Smith, column 5, lines 7-13 and figure 1).

As to claim 15, Smith as modified teaches directing said destination web service via said web content to select production options for producing said imaging data by said production device (Lagarde, column 14, line 62-column 15, line 32).

As to claim 16 as best understood by the Examiner, Smith as modified teaches securely transmitting data (Smith, column 6, lines 31-32).

As to claim 18, Smith as modified teaches:

- a. A user's browser (Lagarde, column 9, lines 10-11) operable to encrypt image data using a first encryption key as part of the encryption process (Smith, column 6, lines 27-39).
- b. Transmitting said encrypted data image (Smith, column 6, lines 27-39).
- c. A destination web service representing a production device (Lagarde, column 15, lines 15-22).

- d. Said web service operable to download said first encryption key into said user's browser (Smith, column 6, lines 28-30, figure 2A and column 3, lines 27-32).
- e. Said web service operable to receive said transmitted encrypted image data and to decrypt said received image data using a private encryption key counterpart of said first encryption key (Smith, column 6, lines 27-39).
- f. A data path interconnection said user's browser with said destination web service (Lagarde, column 9, lines 18-26).

As to claim 19, Smith as modified teaches said production device is a printer (Smith, column 5, lines 7-13 and figure 1).

As to claim 20, Smith as modified teaches said data path is selected from the group consisting of hard wired data paths and wireless data paths (Lagarde, column 9, lines 18-26).

As to claim 21, Smith as modified teaches said first encryption key is a public encryption key (Smith, column 4, lines 45-51).

6. Claims 11, 17 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,151,675 to Smith in view of U.S. Patent No. No. 5,721,908 to

Art Unit: 2134

Lagarde et al. (hereinafter Lagarde) in further view of Applied Cryptography by Bruce Schneier.

As to claims 11, 17 and 22, Smith as modified teaches security measures, but does not expressly mention the use of a session key. However, in an analogous art, Schneier teaches "a hybrid cryptosystem" (page 33, 5th paragraph) wherein a session key is generated that encrypts the data, uses the public key of the recipient to encrypt the session key and sends the session key and data to the destination where the private key counterpart decrypts the session key and the session key decrypts the data (page 33, paragraphs 6-9) in order to more effectively use the computer system resources.

Therefore, it would be obvious to one of ordinary skill in the art at the time of the invention was made to institute the session key encryption scheme, as disclosed by Schneier, as this better utilizes computer resources.

(10) Response to Argument

7. Applicant's arguments, see Appeal Brief, pages 6-24, filed 7/30/2007, with respect to claims 1-22 have been fully considered and are not persuasive.

In response to Applicant's remark that, "the lack of a recitation to an option to not securely transmit data in the independent claim does not make the recitation of an option to print securely in claim 9 or claim 16 indefinite", the Examiner agrees and withdraws the 35 USC 112, 2nd paragraph rejection of those claim 9 and claim 16.

8. In response to Applicant's remark for claim 1 that, "neither Smith nor Lagarde teaches or suggests 'downloading into said browser web content associated with said accessed destination web service'", the Examiner respectfully disagrees. Clearly, the Lagarde patent has a web browser (Lagarde, column 9, lines 9-10) that accesses a web service and downloads web content (Lagarde, column 9, line 66-column 10, line 20). The browser displays the home page of the accessed destination web service that displays menu options for a user to select.

9. In response to Applicant's remark that neither Smith nor Lagarde teach or suggest "where said image data is encrypted using a download[ed] public encryption key from the accessed designated web service and transmitted back to the destination web service", the Examiner respectfully disagrees. It is noted that there is no limitation in claim 1 that refers to a "designated web service." For purposes of this Examiner's Answer, it is assumed that the intended adjective was "destination". The Smith patent downloads the public encryption key from the server associated with the recipient and encrypts a document with the public key of the server for secure transmission (Smith, column 6, lines 28-47). The limitations of claim 1 state that the public encryption key is downloaded from "said accessed destination web service." There is no limitation of "recipient" in the claim language. The recipient of the Smith can be a printer or other production device (Smith, column 5, lines 7-27) of the server associated with the recipient device. The Examiner considers the "receiving server" of Smith to be equivalent to the destination web service of the instant application (Smith, column 4,

lines 56-65). As mentioned above, the recipient can be a printer or other production device and the Applicant makes the same distinction. Looking at claim 14, one can see that public encryption key of the Applicant is associated with the destination web service, not the production device.

10. In response to Applicant's remark that "Smith teaches that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient", the Examiner respectfully disagrees. The Smith patent states, "the server decrypts the document using its corresponding private key, converts the document to a new data representation and then either forwards the document to the recipient inside the firewall, or ... re-encrypts the document" (Smith, column 4, lines 57-61). Clearly, the Smith patent has an option to not re-encrypt the document.

11. In response to Applicant's remark that, "Smith teaches that the approach of not providing a public key of an intended recipient to a browser is preferred over an approach where a public key of a destination web service is provided to a browser", the Examiner respectfully disagrees. Smith does not prefer any embodiment to another. In fact, Smith states, "the server decrypts the document using its corresponding private key, converts the document to a new data representation and then either forwards the document to the recipient inside the firewall, or (in an alternate, ***equally preferred*** embodiment of the invention) re-encrypts the document with the public key of an

intended recipient outside of the firewall or with the public key of another server that is associated with the intended recipient of the document” (emphasis added) (Smith, column 4, lines 57-65). It is clear that the teachings of Smith do not preclude the teaching of “downloading into said browser a public encryption key from said destination web service.”

12. In response to Applicant’s remark that, Smith teaches away from “encrypting a document with a public key of an intended recipient”, the Examiner respectfully disagrees. It is noted that the claim limitations have no recitation of a “public key of an intended recipient.” The claim limitations are directed to a public encryption key of an accessed destination web service. As stated above, the Examiner considers the “recipient” of the Smith patent to be a production device (e.g. printer) and the public encryption key of the server to be equivalent to the public encryption key of the accessed destination web service.

13. In response to Applicant’s remark that, “Lagarde fails to suggest retrieving image data under control of a web browser and transmitting the image data to a destination web service, since Lagarde teaches that agents at a server perform processing tasks in lieu of a browser application”, the Examiner respectfully disagrees. It appears that the Applicant is arguing that “agents at a server perform processing tasks” and not the browser. This contention is directly contradicted by at least the Abstract of Lagarde, “[a] World Wide Web browser makes requests to web servers on a network which receive

Art Unit: 2134

and fulfill requests as an agent of the browser client" (Lagarde, Abstract). The agents work on requests **from** the browser, not in place of the browser. The browser controls the agents that retrieve images and files from the servers. As to the transmission of the image data, that is covered by Smith at column 6, lines 31-32.

14. In response to Applicant's remark that "the cited art fails to teach or suggest at least "choosing desired options represented by said destination web service though said web content", the Examiner respectfully disagrees. The home page of Lagarde has menu options and handles requests of the user. More specifically, "the form of the request can be another form of presentation, as an image, a voice response, or other multimedia presentation" (Lagarde, column 11, lines 8-12). Clearly, the format of the requested report is chosen by the user.

15. In response to Applicant's remark of claims 2-10 that "Smith and Lagarde are devoid of teachings for downloading web content and public key from a destination web service", please refer to section 10; paragraphs 11 and 12, above. In further response to Applicant's remark that, "where the web content is used to prepare a print job containing image data that is encrypted using the public key of the destination web service", the Examiner respectfully disagrees. Lagarde creates reports to be printed (Lagarde, column 14, line 62-column 15, line 32) and in conjunction with the transmission of encrypted documents of Smith satisfies the limitations of claim 10.

16. In response to Applicant's remarks on allowability of claim 12, as the remarks are essentially the same as the remarks for claim 1, they are respectfully traversed for the reasons put forth in Section 10, paragraphs 11-16.

17. In response to Applicant's remark that "claim 16, one of the narrowest claims currently pending, Applicant submits that because of the uniqueness of the claim limitations, claim 16 clearly distinguishes the claimed subject matter over all cited references", the Examiner respectfully disagrees. The limitations of claim 16 are clearly met by the Smith reference. The document to be printed is encrypted and transmitted to the receiving server where it is decrypted behind the firewall and sent to the recipient device for printing (Smith, column 4, lines 45-65). The only option for Smith is to transmit encrypted documents to ensure the security of the transmitted document.

18. In response to Applicant's remark of claim 18 that "neither Smith nor Lagarde teaches or suggests 'a destination web service representing a production device'", the Examiner respectfully disagrees. Lagarde teaches a server with output units that include a printer (a production device) (Lagarde, column 15, lines 16-22). Smith, as well, teaches a recipient of the document can be a printer or fax machine (production units) (Smith, column 5, lines 7-27). In response to Applicant's other remarks on allowability of claim 18, as the remarks are essentially the same as the remarks for claim 1, they are respectfully traversed for the reasons put forth in Section 10, paragraphs 11-16.

19. In response to Applicant's remark that claims 19-21 should be allowed because they contain all the elements and features of the independent claim 18, the Examiner respectfully disagrees. For at least the reasons stated in section 10, paragraph 21, the rejection to claims 19-21 are maintained.

20. In response to Applicant's remark that claims 11 and 17 should be allowed because they contain all the elements and features of the independent claims 1 and 12, the Examiner respectfully disagrees. For at least the reasons stated in section 10, paragraphs 11-16, the rejection to claims 11 and 17 are maintained.

21. In response to Applicant's remark that claim 22 should be allowed because they contain all the elements and features of the independent claim 18, the Examiner respectfully disagrees. For at least the reasons stated in section 10, paragraph 21, the rejection to claim 22 is maintained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

William Powers




KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

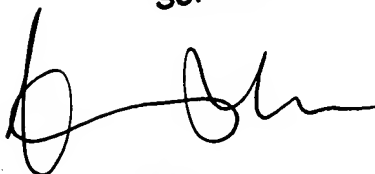
Art Unit: 2134

Conferees:

Kambiz Zand


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Kim Vu



KIM VU
PATENT EXAMINER
TECHNOLOGY CENTER 2100